IB/05/50935

Europäisches Patentamt
European Patent Office
Office européen des brevets

Bescheinigung Certificate Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. Patent application No. Demande de brevet n°

04101304.6

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk

Europäisches Patentamt | European Patent Office | Office européen des brevets

Anmeldung Nr:
Application no.: 04101304.6
Demande no:

Anmeldetag:
Date of filing: 30.03.04
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

Philips Intellectual Property & Standards GmbH

20099 Hamburg
ALLEMAGNE
Koninklijke Philips Electronics N.V.
Groenewoudseweg 1
5621 BA Eindhoven
PAYS-BAS

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se referer à la description.)

Limiting access to personal devices

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)
Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/ Classification internationale des brevets:

G07C9/00

Am Anmeldetag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LU MC NL PL PT RO SE SI SK TR LI

DESCRIPTION

Limiting access to personal devices

The present invention relates to a method of limiting access to a device, said method comprises limiting access to said device according to at least respectively a first and a second level of access. The invention further relates to a device adapted to limit access to said device, said device being adapted for limiting access to said device according to respectively a first and a second level of access.

In today's life a lot of personal mobile devices become more and more capable of storing and handling huge amounts of data. The data ranges from a business presentation on a laptop to music and recordings on an mp3 player on to the personal schedule and the personal address book in a PDA. Most of the data is not meant to be publicly available and should be kept in a safe container. While it is of interest for a user to limit access to a personal device, it is also of interest for the user to enable a predefined group of people to access some of the functionalities and data on the personal device.

WO 0303169 describes a tamper-resistant encoding/obfuscating of software modules where locally stored biometric features/passwords guarantee a high security level for data- and application access. Here, only the user having the correct biometric features can access the data and applications. It is not possible for others to access the data and applications.

It is therefore an object to provide a method to efficiently restrict access to a personal device, which at the same time makes it possible for a predefined group of people to access the device.

This is obtained by a method of limiting access to a device, said method comprises limiting access to said device according to at least respectively a first and a second level of access, wherein said method comprises the steps of:

- receiving a protection key from the rightful user of said device, said protection key comprising a combination of biometric data relating to said rightful user and shareable knowledge data;

- limiting access to said device, whereby a first level of access to said device can be obtained when receiving an access key comprising said shareable knowledge data in said protection key, and a second level of access to said device can be obtained when receiving an access key comprising the combination of said biometric data and said shareable knowledge data in said protection key.

Thereby a device being protected by the biometric data of a rightful user may grant additional access rights to the device for people that at least know the shareable knowledge data. The device could be personal devices such as a PDA, MP3 player, laptop, PC, etc. The rightful user only gives one protection key from which respectively the biometric data and the shareable knowledge data are extracted.

In a specific embodiment limiting access to the device comprises limiting access to data stored on said device, and wherein the data being accessible in said first level of access to said device is encrypted using said protection key based on the combination of said biometric data and said shareable knowledge data. Thereby the data can only be decrypted by the rightful user using an access key comprising both said biometric data and said shareable knowledge data.

In an embodiment limiting access to the device comprises limiting access to data stored on said device, and wherein the data being accessible in said second level of access is encrypted using only said shareable knowledge data in said protection key. Thereby the data can only be decrypted by a user using an access key comprising said shareable knowledge data, thereby being a user to which the shareable knowledge data has been transferred from the rightful user.

In a specific embodiment the protection key is a word, and wherein the biometric data relates to how the word was biometrically received from the rightful user, and

wherein the shareable data is the actual word. This is a simple way of defining a protection key, which can be used by devices either comprising a microphone or where it is possible to attach a microphone.

In specific embodiments said protection key is received via a microphone, a keyboard or a touch screen.

The invention further relates to a device adapted to limit access to said device, said device being adapted for limiting access to said device according to respectively a first and a second level of access, wherein said device comprises:

- means for receiving a protection key from the rightful user of said device, said protection key comprising a combination of biometric data relating to said rightful user and shareable data,

- means for limiting access to said device whereby a first level of access to said device can be obtained when receiving an access key comprising said shareable data in said protection key, and a second level of access to said device can be obtained when receiving an access key comprising the combination of said biometric data and said shareable data in said protection key.

In the following preferred embodiments of the invention will be described referring to the figures, where

figure 1 illustrates a device where different levels of access to the device can be obtained depending on an access key,

figure 2 illustrates how access to a device is limited according to two accessing levels,

figure 3 illustrates how access can be obtained to the device depending on the access key used.

In figure 1 different privacy levels or accessing levels 103, 105, 107 to a device 101 are defined, where access to each level can be obtained depending on an access key 109, 111 provided by the user 113. The accessing level 103 gives full access to the device 101, where full access is illustrated as a circle encircling the whole device 101, and where full access is obtained by using the access key 109. The accessing level 105 gives limited access to the device 101, where the limited access is illustrated as a circle encircling a subpart of the device 101, and where the limited access is obtained by using the access key 111. The accessing level 107 gives further limited access to the device 101, where the further limited access is illustrated as a circle encircling a smaller subpart of the device 101, and where the limited access is obtained without using an access key.

According to the present invention, the accessing keys 109, 111 providing access to the accessing levels are protected by using a combination of biometric data related to the rightful user of the device 101 and shareable knowledge data. Such a combination could e.g. be a spoken word said by the rightful user, where the spoken word said with the similar biometric data or features gives full access 103, and where the correct word said with wrong biometric features gives limited access 105. Further, if a user neither knows the word nor has the right biometric features, the user obtains the further limited access 107 to the device 101. The biometric data related to the spoken word could e.g. be the parameters of the user's eigenvoice representation.

An alternative combination of biometric data and shareable knowledge data could be a word entered using a keyboard by the rightful user, where the biometric features are related to a writing process (e.g. being typing speed, key pressure) for writing the word. A writing process with similar biometric features gives full access 103 to the device 101. Further, if the correct word is written, but with wrong biometric features, a limited access 105 to the device is obtained. Further, if a user neither writes the correct word nor writes it using the right biometric features, the user obtains the further limited access 107 to the device 101.

A further alternative combination of biometric data and shareable knowledge data could be a word written using a touchpad by the rightful user, where the biometric features are related to the writing process (e.g. being how the word is written such as speed, order of letters and how each letter is drawn) for writing the word. A writing process with similar biometric features gives full access 103 to the device 101. Further, if the correct word is written, but with wrong biometric features, a limited access 105 to the device is obtained. Further, if a user neither writes the correct word nor writes it using the right biometric features, the user obtains the further limited access 107 to the device 101.

In figure 2 it is illustrated how access to a device is limited according to two accessing levels. The device initially receives a protection key (R_PK) from the user being the rightful user. The protection key is a combination of biometric data and shareable data as described above, and which could be received from e.g. a microphone, a touch screen or a keyboard either connected to or incorporated into the device. Next, in 202 access is limited to a subpart of actions 203 and data 205 on the device. This subpart is illustrated as the difference between the circle illustrating the limited access 105 and the circle illustrating the further limited access 107 to the device. The data and actions, which are available via the first accessing level L1 are protected, whereby the data and actions are only available when using, as an access key, the shareable data from the combination of biometric data and shareable data in the protection key. Next, in 206 access is further limited to a subpart of actions 207 and data 209 on the device. This subpart is illustrated as the difference between the circle illustrating the limited access 105 and the circle illustrating the further limited access 107 to the device. The data and actions, which are available via the second accessing level L2 are protected, whereby the data and actions are only available when using, as an access key, the combination of biometric data and shareable data from the protection key.

According to the above, access has now been limited to the device in two levels, L1 and L2m, where access to L1 requires an access key according to the shareable knowledge data, and where access to L2 requires an access key according to the combination of biometric data and shareable knowledge data.

In figure 3 it is illustrated how access can be obtained to the device depending on the access key used. In 301 the device receives an accessing key from the user 300. Next, the device checks whether the accessing comprises both the biometric data and the shareable knowledge data, and if this is the case, full access 103 to data and actions on the device is allowed, since the user 300 is the rightful user. If both the biometric data and the shareable knowledge data are not comprised in the access key, then in 305 it is checked whether at least the shareable knowledge data is comprised, and if this is the case limited access 105 to data and actions on the device is allowed, since the user is a person trusted by the rightful user, who has received the shareable knowledge data from the rightful user. If neither the biometric data nor the shareable knowledge data is comprised in the access key, then further limited access 107 is allowed, since the user is neither the rightful user nor a person trusted by the rightful user.

More specifically, the above could be explained as whenever a device is acquired or legally transferred to a new owner biometric features for the new owner is gathered and a robust combination thereof is converted via a one way hash function (MD5, SHA-1, RIPEMD-160 or similar ones) into a user access key that is used to identify the user/owner, allow or decline access to the device according to the second accessing level, and to encrypt and decrypt stored data (via DES, 3DES, RC5 or newer variants or encryption routines). The two sets of features for identifying users/granting access rights and for encryption/decryption should have no overlap, since the identifying features are stored on the device, whereas the encryption key should not be stored. In another variant of the invention the identifying features are stored encrypted using the complementary set of features that is not stored but created session-wise on the fly (e.g. the user utters a greeting phrase and characteristic parameters. In another variant of the invention the identifying features are stored encrypted using the complementary set of features that is not stored but created session-wise on the fly (example: the user utters a greeting phrase, and characteristic parameters of the best matching eigenvoice of an automatic speech recognition process are used to encrypt the recognized word). When no further action is taken by the user, all data is stored this way encrypted with a key that is very

specific for each single user and not stored in any way. The user/owner may grant additional access rights for people that at least know the greeting phrase ("friends/family", the plain text of e.g. the greeting phrase does match, but the encrypted version does not) or everybody else ("world", neither the phrase is known nor could the encrypted version be matched with a stored reference) and use these three different levels of privacy without having to deliberately define and maintain a list of more or less privileged users. On top of this generic user classification in "owner", "friends" and "others" one can establish a more detailed rights administration combining user specific signatures and e.g. more or less secret pass-phrases if necessary. In another variant of the invention the data might be encrypted and stored twice using the user's private key and a master key in parallel to have a backdoor to the data in case this is appropriate (e.g. an employee's company related data should be readable using a company-master-key or a child's toy doll should answer mother's questions).

It should be noted that the above-mentioned embodiments illustrate rather than limit the invention, and that those skilled in the art will be able to design many alternative embodiments without departing from the scope of the appended claims. In the claims, any reference signs placed between parentheses shall not be construed as limiting the claim. The word 'comprising' does not exclude the presence of other elements or steps than those listed in a claim. The invention can be implemented by means of hardware comprising several distinct elements, and by means of a suitably programmed computer. In a device claim enumerating several means, several of these means can be embodied by one and the same item of hardware. The mere fact that certain measures are recited in mutually different dependent claims does not indicate that a combination of these measures cannot be used to advantage.

CLAIMS

1. A method of limiting access to a device, said method comprises limiting access to said device according to at least respectively a first and a second level of access, wherein said method comprises the steps of:

- receiving a protection key from the rightful user of said device, said protection key comprising a combination of biometric data relating to said rightful user and shareable knowledge data,
- limiting access to said device whereby a first level of access to said device can be obtained when receiving an access key comprising said shareable knowledge data in said protection key, and a second level of access to said device can be obtained, when receiving an access key comprising the combination of said biometric data and said shareable knowledge data in said protection key.

2. A method according to claim 1, wherein limiting access to the device comprises limiting access to data stored on said device, and wherein the data being accessible in said first level of access to said device is encrypted using said protection key based on the combination of said biometric data and said shareable knowledge data.

3. A method according to claim 1-2, wherein limiting access to the device comprises limiting access to data stored on said device, and wherein the data being accessible in said second level of access is encrypted using only said shareable knowledge data in said protection key.

4. A method according to claim 1-3, wherein the protection key is a word, and wherein the biometric data relates to how the word was biometrically received from the rightful user, and wherein the shareable data is the actual word.

5. A method according to claim 1-4, wherein said protection key is received via a microphone.

6. A method according to claim 1-5, wherein said protection key is received via a keyboard.

7. A method according to claim 1-5, wherein said protection key is received via a touch screen.

8. A device adapted to limit access to said device, said device being adapted for limiting access to said device according to respectively a first and a second level of access, wherein said device comprises:

- means for receiving a protection key from the rightful user of said device, said protection key comprising a combination of biometric data relating to said rightful user and shareable data,
- means for limiting access to said device, whereby a first level of access to said device can be obtained when receiving an access key comprising said shareable data in said protection key, and a second level of access to said device can be obtained, when receiving an access key comprising the combination of said biometric data and said shareable data in said protection key.

ABSTRACT

Limiting access to personal devices

The present invention relates to a method of limiting access to a device, said method comprises limiting access to said device according to at least respectively a first and a second level of access, wherein said method comprises the steps of:

- receiving a protection key from the rightful user of said device, said protection key comprising a combination of biometric data relating to said rightful user and shareable knowledge data,
- limiting access to said device, whereby a first level of access to said device can be obtained when receiving an access key comprising said shareable knowledge data in said protection key, and a second level of access to said device can be obtained, when receiving an access key comprising the combination of said biometric data and said shareable knowledge data in said protection key.

Thereby a device being protected by the biometric data of a rightful user may grant additional access rights to the device for people that at least know the shareable knowledge data. The device could be personal devices such as a PDA, MP3 player, laptop, PC, etc.

(Fig. 1)

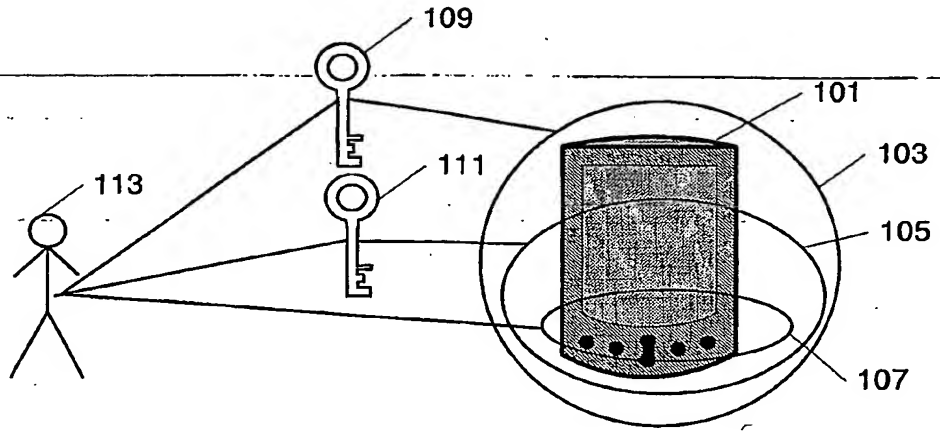

Fig. 1

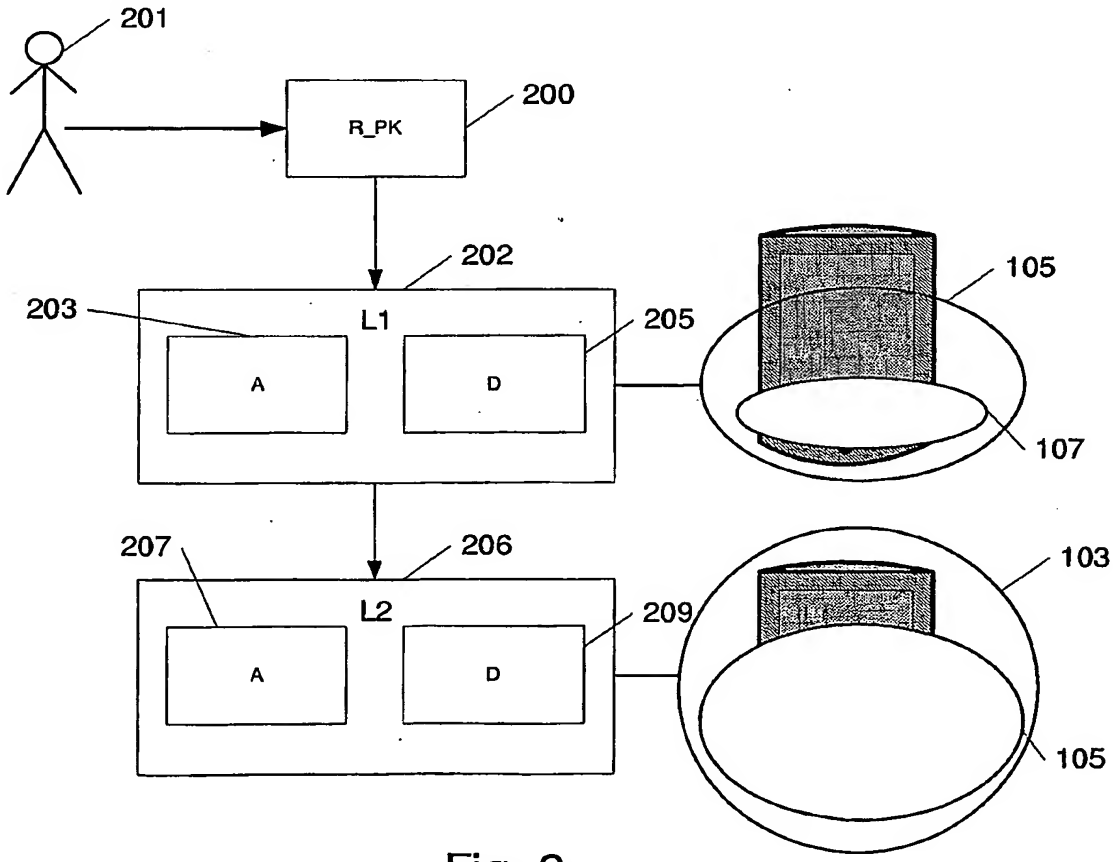

Fig. 2

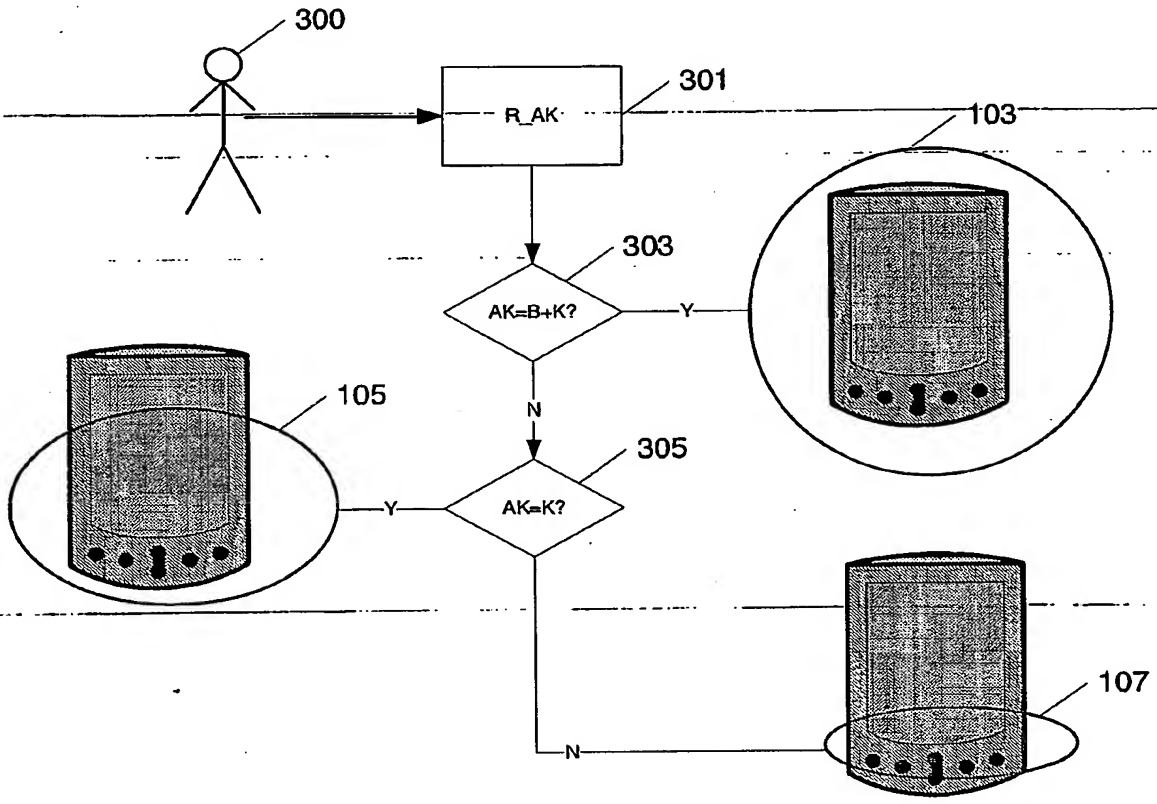

Fig. 3